

# 키스트로크를 이용한 모바일 오피스 사용자 인증 방식

이중혁, 최옥경, 예홍진  
아주대학교 대학원 지식정보보안학과  
e-mail: [yahssap@ajou.ac.kr](mailto:yahssap@ajou.ac.kr), [okchoi@ajou.ac.kr](mailto:okchoi@ajou.ac.kr), [hjveh@ajou.ac.kr](mailto:hjveh@ajou.ac.kr)

## Mobile Office Authentication Method using Keystroke

Jong-Hyeok Lee, Okkyung Choi, Hong-Jin Yeh  
Dept of Knowledge Information Security, Graduate School of Ajou University

### 요 약

스마트폰이 발전함에 따라 모바일 단말기를 이용해 외부에서 회사 업무를 처리할 수 있는 모바일 오피스 업무 시스템이 증가 하고 있는 실정이다. 개인 휴대 기기의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난, 분실 할 수 있으며 이에 따라 개인 및 기업의 정보 유출이 가능하다. 그러므로 본 방식 연구에서는 모바일 오피스 환경에 보다 효율적이고 정보보호를 위한 인증 방법으로 키스트로크(KeyStroke) 방식과 모바일의 IMSI / IMCI 방식을 연구 분석하여 강력하고 적합한 인증 방식을 제안한다.

### 1. 서론

모바일 기기의 보편화와 다양한 종류의 모바일 기기들의 등장에 따라 각종 모바일 서비스들이 제공되고 있다. 통화기능은 물론 이메일, 인터넷, 전자책 등을 활용할 수 있는 소형 컴퓨터 기능을 갖춘 멀티 휴대 전화로 전 세계 스마트폰 시장은 점차 확대 되고 있으며 더 나아가 언제 어디서나 모바일 단말기를 통해 외부에서 회사 업무를 처리할 수 있는 모바일 오피스 업무 시스템이 증가 하고 있는 상황이다. 개인 휴대 기기의 특성상 이용자의 부주의로 인해 기기 및 메모리카드 등을 도난, 분실 할 수 있으며 이에 따라 개인 정보 유출이 가능하며 기업의 기밀정보 유출도 가능하다. 이런 개인정보를 보호하는 사용자 인증이 매우 중요하나 현재 보편적으로 사용되는 개인 식별번호 입력 방법 또는 패스워드 입력 방법은 엿보기 공격(Shoulder Surfing Attack: SSA)에 안전하지 못하기 때문에 공격자는 쉽게 사용자의 정보를 얻을 수 있다. 기존의 이러한 SSA를 막기 위한 방법들이 제안되어 왔으나 사용편의성이 떨어지고 모바일 환경에서 사용하기 힘든 단점이 있었다. 이러한 문제점을 해결하기 위한 방안으로 생체 인식 방법이 제안되어 왔다. 생체 인증은 신체의 일부부분이므로 분실 위험이 적으며, 접근 카드에 비해 상대적으로 복제나 강탈 위험이 적다는 장점이 있다. 하지만 생체 인식 방법으로는 여러 가지 단점이 발생하게 된다. 지문인식 같은 경우는 값싸고 단순하며 가장 널리 사용되는 방식이지만 복제가 가능하고 다수인 경우 정밀도가 떨어지는 단점을 보이며, 홍채 인식방법은 사람마다 독특한 눈동자의 컬러 부분 패턴 인식으로 인증 하는 것으로 사용자의 거부감 및 신체적으로 불편함을 느낄 수 있게 된다. 얼굴 인식 인증 방법은 카메라에 찍힌 얼굴의 특징으로 인증 하

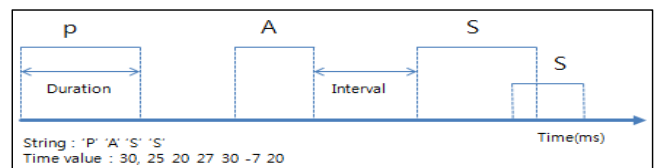
는 방법이지만 조명 상태에 따라 매우 민감하다는 단점이 있다 음성인식은 오류율이 높고 녹음에 의해서 무력화 가능성이 높다, 다시 말해서 이런 생체인식 방법들은 비용, 정확성, 사용자 거부감 등의 문제가 남아있다. 본 연구에서는 생체 인식 중에서 이러한 문제를 최소화 시킬 수 있는 키스트로크 인증 방식을 응용하여 제안함으로써 보다 강화된 사용자 인증 서비스를 제공한다.

### 2. 관련연구

#### 2.1. Keystroke

##### 2.1.1. 인증방식

키스트로크 인증 방식(Keystroke dynamic)은 사용자가 타이핑하는 습관이나 독특한 특징을 로깅하여 분석한 다음 적법인 사용자인가를 분석하는 것을 말한다. 키스트로크 인증은 휴대 단말기의 짧은 암호 사용의 문제점을 극복하기 위해서 비밀번호의 일치성과, 패턴유형을 조합 하여 다양한 인증 값을 도출 할 수 있게 하였다. 다시 말해서 키스트로크 패턴 기반의 사용자 인증은 개인마다 키스트로크 패턴이 다르다는 연구 결과에 착안하여, 암호의 내용뿐만 아니라, 암호의 키스트로크 패턴까지 이용한 사용자 인증 방식이다. 즉, 암호가 유출되어 일차적인 보안망을 통과 하더라도 키스트로크 패턴까지 검사하여 침입을 방지할 수 있게 된다[1].

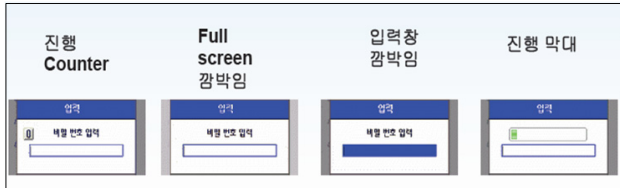


(그림 1) Keystroke 인증

'PASS'라는 문자열을 입력하게 되면 문자열값과 입력한 시간 값이 측정되어 인증 값들이 산출된다.

### 2.1.2. 템포 큐

템포 큐란 사용자가 암호를 입력할 때 일정한 간격으로 사용자에게 신호를 보내주는 방식으로 시각 큐, 청각 큐, 시청각 큐가 있다. 시각 큐는 시각적으로 일정한 시간동안 화면을 깜박인다거나 진행 바를 두어 사용자가 템포를 인식 시켜주는 역할을 하며, 청각 큐는 일정한 시간마다 비트음을 주거나 음악을 넣어 사용자가 인식하는데 도와주는 역할을 한다[2].



(그림 2) 시각 큐

## 2.2. IMSI / IMEI 인증

IMSI는 국제 모바일 가입자 인증번호로써 GSM 이동 통신망에서 통신 가입자에게 할당되는 구체적으로 유일한 식별번호이다. IMSI는 모바일에 장착되는 USIM카드에 저장되어 있으며 교환이 가능하다.

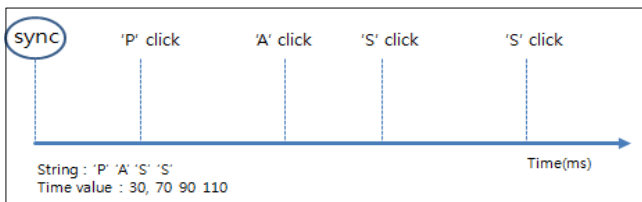
IMEI는 제조사가 전 세계의 수많은 휴대전화를 구별하기 위해 만든 휴대폰 고유의 번호가 있는데 이것을 IMEI라고 한다.

이 두 가지 방식을 가지고 적용하게 되면 데이터베이스에 등록 된 기기와 USIM칩이 일치해야 인증에 성공하게 된다[3].

## 3. 설계 및 연구 방안

### 3.1. Keystroke 설계 방안

키스트로크 인증은 키보드에서 주로 사용하는 방식으로 적은 양의 문자열을 사용하는 스마트폰에 적용하기에 그 효과를 보기 어렵다. 그래서 간편하면서 정확성을 높이기 위한 키스트로크 방식을 (그림 3)과 같이 설계 하였다.



(그림 3) 스마트폰에 적합한 Keystroke 설계

Sync key를 두어 시간 값과 템포 큐를 동기화 시켜주고 시간 값은 Stopwatch의 원리로 문자열 하나씩 클릭을 할 때마다 시간값을 저장해 하여 각 문자열과 같이 서버에 보내게 되는 방식이다. 이때 DB에 저장 해 놓은 문자열과 시간 값을 비교를 한다. 시간은 1/1000초 단위이기 때문에 인증 오차의 허용치 즉, 임계값을 설정 해 준다. 임계값 범위 안에서 오차를 허용하였을 때와 문자열이 일치하였

을 때 인증은 성공, 두개 요소 중에 하나라도 일치하지 않는다면 인증은 실패하게 된다.

## 3.2. 연구 방안

### 3.2.1. 데이터 획득 방법

- 데이터 구성을 practice의 집합으로 분류하여 추출한다.
- 서버 측에 입력된 값과 등록된 값과의 오차를 나타낸다.
- 데이터는 진동 큐, 시각 큐, 그리고 템포 큐가 주어지지 않았을 때에 3가지 상황 내에서 각각 수집 한다.
- 임계값의 오차 허용치를 변경 해주며 수집 한다.
- 템포 큐에 대한 반응속도를 측정 할 수 있도록 한다.
- 성별, 나이, 스마트폰 사용여부에 따른 분석 실시한다.
- 평가를 위해 사용자들에 대한 시스템 친밀도를 높이고, 시스템에 대한 정확도를 높이기 위해 몇 분간의 학습기간을 가지고 실험을 시행할 것이다. 다음과 같은 방법으로 수행한다.
- FRR 위해 각 사용자에게 대한 genuine attempt를 수행
- FAR 위해 각 사용자에게 대한 imposter attempt를 수행
  - ① 문자열만 알고 있는 환경에서 테스트
  - ② 문자열과 패턴을 알고 있는 환경에서 테스트.
- 테스트 시 실험은 진동 큐, 시각 큐가 주어졌을 때와 그리고 템포 큐가 주어지지 않는 3가지 상황과 민감도를 바꿔가며 수회 반복적 연습 후 Practice 실시하며 (표 1)과 같은 평가 항목을 측정한다.

(표 1) 평가항목

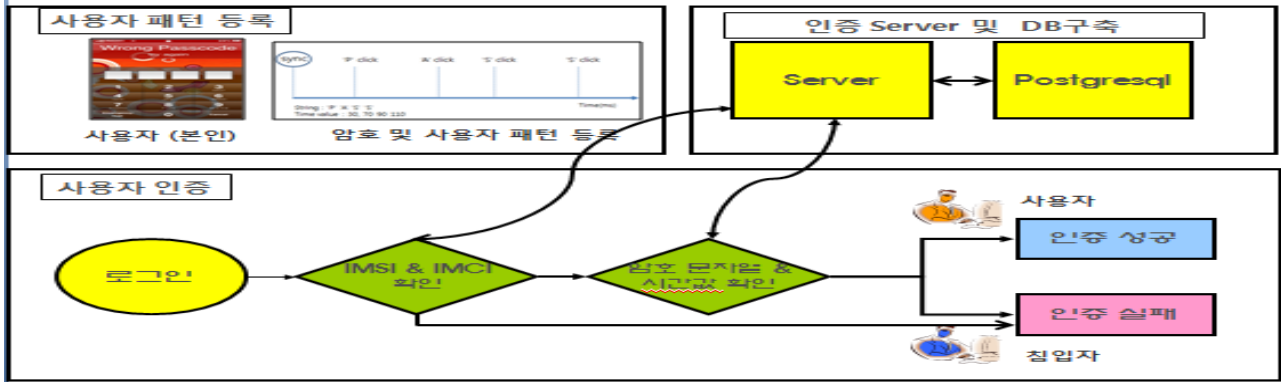
평가항목	평가내용
FRR	데이터가 일치하거나 거부하는 비율
FAR	데이터가 일치하지 않으나 수락하는 비율
EER	FAR과 FRR 데이터가 일치 할 때의 오류 비율

- 환경
  - ① 모든 실험은 고정 IP가 할당 된 야외환경과 필드 환경에서 진행.
  - ② 오프라인 환경에서 테스트.
- 최초 Password를 등록 시 저장 된 문자열과 패턴은 DB에 저장, 이후 실험 되는 수행 값과 인증 성공여부는 서버에서 확인하여 기록표에 기입한다.

이름 : 홍길동	나이 : 28	스마트폰 사용여부 : 0	비교(인증성공여부)			
성별 : (남) 여						
비밀번호 문자열 값	1	2	3	4		
비밀번호 시간백터 값	2,034	4,556	7,321	8,011		
민감도 (고) (임계값 ±0.1초)	시각 큐	2,124	3,056	7,460	8,809	X
	진동 큐	2,034	4,455	7,229	7,989	O
	템포 큐 X	2,530	5,596	6,361	8,419	X
민감도 (중) (임계값 ±0.5초)	시각 큐	2,334	4,156	6,921	8,381	O
	진동 큐	2,834	5,036	7,621	8,411	O
	템포 큐 X	2,434	5,056	6,721	7,711	X
민감도 (저) (임계값 ±1초)	시각 큐	2,134	4,476	7,227	8,107	O
	진동 큐	2,731	4,656	7,341	7,911	O
	템포 큐 X	2,294	4,596	7,321	7,021	O

(그림 4) 데이터 기록표

### 3.2.2. 시스템 설계



(그림 5) 키스트로크를 이용한 모바일 오피스 사용자 인증 시스템 구조

(그림 5)은 키스트로크 이용한 모바일 오피스 사용자 인증 시스템 구조를 나타낸다. 모바일의 UI에 패스워드를 입력하게 되면 서버는 스마트폰의 기기일련번호와 USIM칩의 고유번호를 확인을 한다. 일치하면 문자열과 키스트로크 시간값을 확인하게 되고 인증 성공 여부가 가려지게 된다.

## 4. 결론

일반적으로 키스트로크 인증 방식은 키보드 사용자 대상으로 한 것이며, 인증의 일관성을 향상하기 위해 템포 큐로 시각 큐와 청각 큐를 사용하였다. 본 논문에서는 모바일 사용자를 대상으로 연구를 하며, 그 특성에 맞는 템포 큐 즉, 진동 큐에 대해 제안한다. 또한 키스트로크의 duration과 interval을 즉각적인 click 시간으로 대체하여 모바일의 적합한 키스트로크 방식을 구현 한다. 또한 IMSI와 IMEI 방식으로 기기분실 및 USIM 도난에 대한 대책을 연구하여, 모바일 오피스 환경에서 인증의 정확성과 효율성 그리고 보안성을 구현 분석 한다.

### 참고문헌

[1] Cho, S. and Hwang, S. (2006). Artificial rhythms and cues for keystroke dynamics based authentication, Lecture Notes in Computer Science (LNCS) 3832: 626-632.  
 [2] Hwang, S., Lee, H. and Cho, S. (2009b). Improving authentication accuracy using artificial rhythms and cues for keystroke dynamics-based authentication, Expert Systems with Applications, In press.  
 [3] 박희영(2009.11) “IMSI 및 IMEI와 휴대전화의 위치 확보의 합헌성 여부“ 법제처, [MGL] 월간 법제 월간법제